

ePolicy Orchestrator (ePO) Installation Document

Table of Contents

ePolicy Orchestrator (ePO) Installation Document	1
Table of Contents	1
Scope of Document and Direction for Districts.....	3
Executive Summary	3
Infrastructure Considerations.....	4
Pre-Installation	6
Installation of Microsoft SQL Server	9
Installing Microsoft SQL Server 2000 program	9
Installing Microsoft SQL Server 2000 SP3a Patch.....	10
Installing Microsoft SQL Server 2000 with SP3a Hotfixes.....	11
Installing MS03-031 Hotfix	11
Installing KB826161 Hotfix	11
Installation of ePolicy Orchestrator 3.0.2a	12
Installation of ePO on the Server	12
Installing ePO v3.0.1.....	12
Updating ePO v3.0.1 to ePO 3.0.2a.....	13
Updating ePO to Patch 6.....	14
Installing ePO Remote Management Console on a Workstation.....	14
Installing the ePO Management Console v3.0.1	14
Updating the ePO v3.0.1 Management Console to the ePO 3.0.2a Management Console	15
Updating ePO to Patch 6.....	15
Configuration of ePO Server	16
Pre-Configuration Tasks	16
Starting ePO for the First Time.....	16
Creating a Global Administrator user for OET.....	16
Installing EPO Agent Patch 7	17
Configuring the Repository.....	17
Adding the VirusScan Enterprise v7.1 Program Files	17
Adding the VirusScan v4.51 Program Files	18
Installing the CorrectENG.EXE update.....	19
Configuring Proxy Settings for Pulling DAT Updates from NAI	19
Creating Task to Pull DAT Updates from NAI	19
Manually Pulling the DAT File from NAI	20
Setting Program Policies.....	20
ePolicy Orchestrator Agent Configuration	20
VirusScan Software	21
VirusScan Enterprise v7.1 Workstation settings	21
VirusScan Enterprise 7.1 Server Settings	23
VirusScan 4.5.1 Settings.....	25
Creating Agent Installation Package.....	27

Setting up the Directory	27
Adding the District Site	27
Adding the Server group	28
Adding the Workstations group	29
Adding the Win9x Group	30
Testing Directory IP Configuration	30
Sorting Computers by IP Address	31
Inactive Agent Maintenance Task	32
Setting Up the DAT File Update Task	32
Setting Up the Emergency DAT Update Task	33
Setting up Installation Tasks	34
VirusScan v7.1 Installation (for Window NT 4.0, 2000, XP, and 2003 clients)	34
VirusScan v4.51 Installation (for Windows 95 and 98 clients)	34
Installing the ePolicy Orchestrator Agent on Servers	35
Setting up Network to Deploy ePolicy Orchestrator Agent	36
Setting Up Logon Script	36
Verification of Services	38
Verifying ePolicy Orchestrator 3.0 Agent Installation	38
Checking the Status of the EPO Agent	39
Maintenance Tasks	40
Searching and Moving Windows 9x machines to the Win9x Group	40
Sorting Computers by IP Address	41

Scope of Document and Direction for Districts

This document is provided as guidance to school districts pertaining to the district-level implementation of NAI's Enterprise Policy Orchestrator (ePO) as part of Project Safety Net. The intent of this document, and all, contents are to define the recommended actions in order for school districts to effectively deploy this technology at a local level.

Districts are asked to take the following actions upon receipt of this document:

- 1) Review this document in its entirety and become familiar with its contents. The district CIO and technical support staff represent the primary target audience.
- 2) Contact their respective KETS Engineer or the KETS Help Desk with any questions, comments, or concerns.

Executive Summary

Project Safety Net was identified by the KETS Engineer Team, as a high priority OET/SNS service delivery improvement goal for the beginning of the 2004 School year. The core objective developed by the SNS Security Committee: ***To minimize the impact of viruses and worms to the school districts at the start of the school year 2004.***

The business reasons driving this project include reducing the loss of instruction time for the school districts, reducing labor overtime cost for the school district and OET SNS, preventing a loss of focus on overall customer service because of a catastrophic event, and maintaining the confidence of the school districts in the reliability of the KETS network.

At the start of school over the past three school years the loss of Internet instructional time for Kentucky school districts has been significant. One of the primary reasons for this loss of Internet access is that school districts normally power down their workstations as part of the cleaning process during the summer break period. When the workstations are re-connected back to the network for the start of school, they are exposed to new viruses and worms that have been propagated during the down period.

The reactive effort to clean the workstations and restore the network to operation requires a tremendous amount of work by school district technical personnel and SNS staff. As an example, in 2003, approximately 118 virus related help desk tickets were identified during the August/September time frame. SNS technical personnel worked approximately 500 hours of overtime during this period plus additional hours worked by the district technical staffs. School districts and OET SNS are not staffed for nor budgeted for this type of peak demand for technical labor.

Because of the focus and effort required to restore network operation, the overall focus on customer service by SNS is diminished. Significant effort is required to catch up on other service related issues and provide timely responses to new issues impacting the

network. Internal service delivery improvement projects at both the district level and at the OET level must also be placed on hold while technical resources react to the immediate impact of a virus infection.

This type of catastrophic event causes a loss of confidence in the KETS network. The end result of this loss of confidence being reduced use of the network for instruction. The scope of Project Safety Net includes six major activities:

- Activity 1 – Communicate end of school/start of school KETS supported requirements to the school districts.
- ***Activity 2 – Develop district level KETS supported EPO standards and develop a joint OET/school district plan to implement district level EPO for all school districts connected to the KETS network. (This effort will also include providing protection for Macintosh workstations to the degree it is available)***
- Activity 3 – Development and implementation of a functional virus alert process that originates within SNS.
- Activity 4 – Implement EPO for KDE users.
- Activity 5 – Implementation of SUS in the remaining districts (approximately 98) based on KETS supported standards.

Infrastructure Considerations

The following topics should be carefully reviewed before deploying ePO within your school district. These are “make-or-break” issues which, if the incorrect decision is made, can directly affect the effectiveness and/or success of your ePO deployment.

- Consideration should be given to ePO repository placement in relation to a school district’s internal network design. Any school district with an internal fiber network or an internal point-to-point T1 network (not including frame T1’s) will not need any repositories at school or remote office sites. Any school district with an internal network consisting of frame T1’s, fractional T1’s, or low-end wireless network will need to place a repository at the end of each of those network links.
- Consideration should be given to the number of workstations within a school district which are using the services provided by ePO. Any school district with over two-thousand workstations must use a Microsoft SQL Server 2000 as a back-end database system. Any school district with under two-thousand workstations can use MSDE, which comes bundled as a convenience, with ePO.

- Consideration should be given to the specifications of the server on which ePO is going to run. The minimum recommended specifications for the ePO server are as follows:
 - Windows Server 2003 Standard Edition
 - Pentium III 1GHz processor
 - 1GB RAM
 - 2GB of free disk space
 - 1024x768, 256 color, VGA monitor

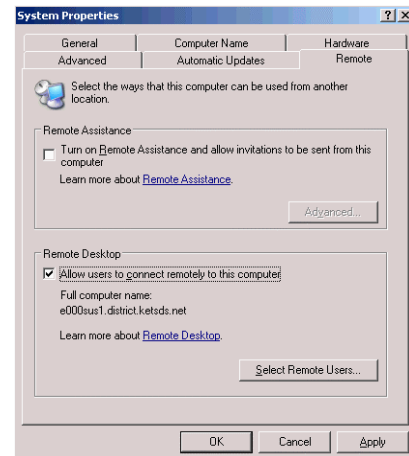
- Consideration should be given to the specifications of the server if ePO and Microsoft SQL Server 2000 are going to run on the same machine. The minimum recommended specifications for this dual-purpose server is as follows:
 - Windows Server 2003 Standard Edition
 - Pentium III 1GHz processor
 - 2.5GB RAM
 - 10GB of free disk space
 - 1024x768, 256 color, VGA monitor

- Consideration should be given to the specifications of the separate server, if necessary, on which Microsoft SQL Server 2000 is going to run. The minimum recommended specifications for the Microsoft SQL Server 2000 are as follows:
 - Windows Server 2003 Standard Edition
 - Pentium III 1GHz processor
 - 1.5GB RAM
 - 8GB of free disk space
 - 1024x768, 256 color, VGA monitor

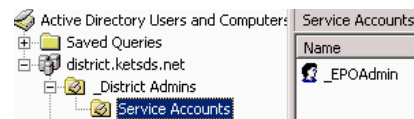
Pre-Installation

1. Prepare a server, with the minimum specifications as listed above, with Windows 2003 Server and the latest operating system patches installed
2. Turn on Remote Desktop for the EPO/SUS server by doing the following:

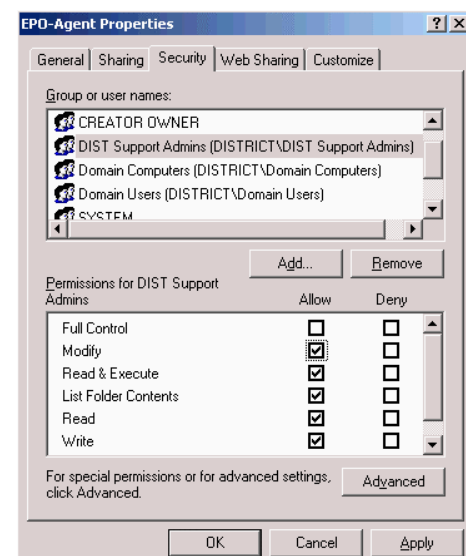
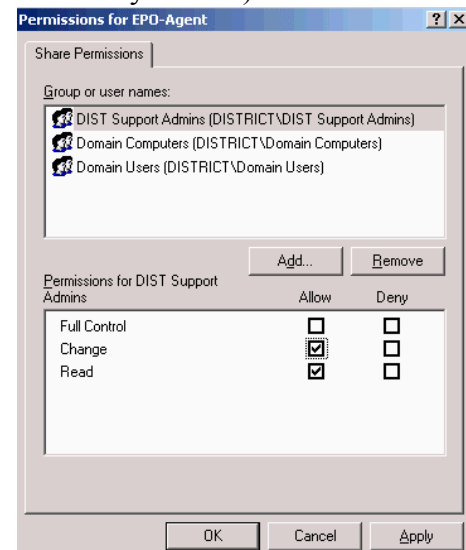
- a. Logon to the EPO/SUS Server
- b. Right click on “My Computer”
- c. Click on “Properties”
- d. At the “System Properties” screen, click on the “Remote” tab
- e. Under “Remote Desktop” at the bottom, check “Allow users to connect remotely to this computer”
- f. At the warning screen, click “OK” (it warns that accounts that use Remote Desktop need to have passwords)
- g. At the “System Properties” screen, click “OK”



3. Add “OET Security Group” to Administrators groups of the EPO/SUS Server: (This will allow some of the OET staff to Remote Desktop to the EPO/SUS server to help troubleshoot any issues with EPO)
 - a. Logon to the EPO/SUS Server
 - b. Right click on “My Computer”
 - c. Click on “Manage”
 - d. At the “Computer Management” screen, double click on “Local Users and Groups”
 - e. Double click on “Groups”
 - f. In the area on the right, double click on “Administrators”
 - g. At the “Administrators Properties” screen, click on “Add”
 - h. Under “Enter the object names to select”, type in “**KETS\SUS EPO Admins**”
 - i. Click “OK”
 - j. “OET Security Group” should be added to the list
 - k. Click “OK” to complete
4. Install Microsoft SUS as described in the documentation provided by OET (Final Standards Document for SUS can be downloaded at <http://www.education.ky.gov/KDE/Administrative+Resources/Technology/KETS+Help+Desk/How+Tos+and+Standards+Documents/KDE+Private+IP+Implementation+Plan+.htm>)
5. Need to create an EPO service account named “**_EPOAdmin**”. It should be under “District Admins” in the “Service Accounts” OU and in the following groups:
 - a. DIST Support Admins



- b. When creating the account, you should uncheck “Change Password at Next Logon”, check “User cannot change password”, and check “Password does not expire”
 - c. Note: Only District Technology administrator should know this passwords and it should not be shared with anyone.
6. Need to have a Windows XP with SP1 workstation to load the EPO Remote Management Console. It should have Internet Explorer 6.0 or higher installed and Microsoft Java Virtual Machine (MSJVM) or Sun Java (available at <http://www.java.com/en/download/manual.jsp>) loaded.
7. Download the EPO Installation CD by clicking the following link: <ftp://ketsftp.k12.ky.us/epo/epo-cd12.iso>
8. Burn the ISO image to a CD (it is highly recommended that you use CD Burning software such as Roxio Easy CD Creator or Nero).
9. On the EPO server, do the following to create the EPO-Agent share:
 - a. Create a folder on the C:\ drive and name it “EPO-Agent”
 - b. Right click the EPO-Agent directory and select “Sharing and Security...”
 - c. Click on the “Sharing” tab (should be selected by default)
 - d. Click on Share this folder and in the “Share name” field, enter EPO-Agent (this should be entered by default)
 - e. Click on the Permissions button at the bottom
 - f. At the “Permissions for EPO-Agent” screen, select “Everyone” and click “Remove”
 - g. At the “Permissions for EPO-Agent” screen, click Add and enter “Domain Users; Domain Computers; DIST Support Admins”
 - h. Click “OK”
 - i. Click on DIST Support Admins and in the bottom section underneath “Allow” check “Change”
 - j. Click “OK”
 - k. In the “EPO-Agent Properties” screen, click on the “Security” tab
 - l. Click on “Add”
 - m. In the “Select Users, Computers, or Groups” screen, enter “Domain Users; Domain Computers; DIST Support Admins”
 - n. Click “OK”
 - o. Click on DIST Support Admins and in the bottom section underneath “Allow” check “Modify”



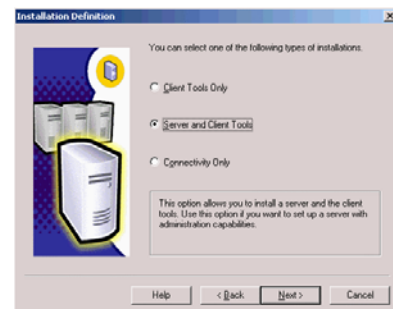
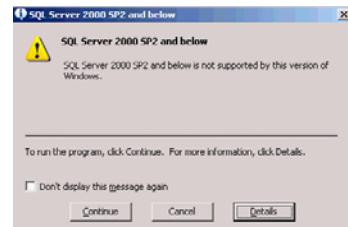
- p. Click “OK”
- 10. Copying files to EPO-Agent share:
 - a. Insert the EPO Installation CD in the CD-ROM drive (of the EPO/SUS server if you are doing this at the server console or through Terminal Services, but the CD-ROM drive of the workstation if you are remotely copying the files)
 - b. Click on Start -> Run
 - c. In the “Open” field, enter “D:\Copy to EPO Agent Share\”
 - d. Click on “OK”
 - e. Copy everything in that directory into the EPO network share you created earlier. It should contain
 - i. 451SP1UPD (a folder with the files to load SP1 for VirusScan 4.51)
 - ii. EPO2KXP.BAT (this is the script that loads the agent on Windows 2000 and Windows XP workstations)
 - iii. ChkePOAgent.vbs (this is a script that verifies if the ePO Agent is already loaded on Windows 2000 and Windows XP workstations)
 - iv. DCOM95.exe
 - v. DCOM95lg.epo
 - vi. DCOM98.exe
 - vii. DCOM98lg.epo
 - f. Right click “EPO2KXP.BAT” and select properties and make sure that the Read-Only box is **Unchecked**
 - g. Click on “OK”
 - h. Right-click “EPO2KXP.BAT” and select “Edit”
 - i. Search for any instances of “E000SUS1” and replace it with the name of your EPO/SUS server (there should only be 2 instances)
 - j. Save the changes and close any open windows
- 11. Have a list of the Active DHCP Scopes or the Private IP Address allocation sheet printed out and available during the installation process. If you don’t know or do not have this information, please contact your KETS Engineer for assistance.
- 12. E-mail your KETS Engineer and request that you have the EPO Agent Group Policy Object created under the Workstations OU. Have the EPO/SUS Server name, the full path to the EPO-Agent share (i.e. [\\E000SUS1\EPO-Agent](#)), and the IP Address of the EPO/SUS Server

Installation of Microsoft SQL Server

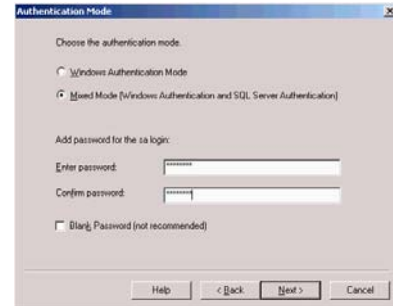
Note: This section is only for districts with more than 2000 workstations. They will need to install Microsoft SQL Server 2000 before they can load ePolicy Orchestrator. All other districts can skip to page 10 to start installing ePolicy Orchestrator.

Installing Microsoft SQL Server 2000 program

1. Login to the EPO/SUS Server
2. Insert the SQL Server 2000 CD
3. The CD should autorun and a Microsoft SQL Server 2000 screen should pop-up
4. At this screen, click on “SQL Server 2000 Components”
5. At the next screen, click on “Install Database Server”
6. A screen named “SQL Server SP2 and below” will pop-up stating “SQL Server 2000 SP2 and below is not supported by this version of Windows.”
7. Click on “Continue”
8. At the “Welcome to the Microsoft SQL Server Installation Wizard” screen, click “Next”
9. Click on “Local Computer”
10. Click “Next”
11. Click on “Create a new instance of SQL Server, or install Client Tools”
12. Click “Next”
13. Fill out the “Name” and “Company” fields
14. Click “Next”
15. At the “Software License Agreement” screen, click “Yes”
16. At the “Installation Definition” screen, click on “Server and Client Tools”
17. Click “Next”
18. At the “Instance Name” screen, make sure that “Default” is checked
19. Click “Next”
20. At the “Setup Type” screen, click on “Typical”
21. Click “Next”
22. At the “Services Accounts” screen, click on the following:
 - a. At the top, click on “Use the same account for each service. Auto start SQL Server Service.”
 - b. Under “Service Settings”, click on “Use the Local System account”
23. Click “Next”



24. At the “Authentication Mode” screen, click on “Mixed Mode (Windows Authentication and SQL Server Authentication)”
25. Then under “Add password for the sa login:”, it will prompt you to enter and confirm a password (The **sa** account is the default database Administrator account.)
26. Click “Next”
27. At the “Start Copying Files” screen, click “Next”
28. At the “Choose Licensing Mode” screen, do the following under “Licensing Mode”:
 - a. Click on “Per Seat for”
 - b. Enter the number of Remote Management Consoles you will plan on connecting to the EPO Server. (These should be covered by your STI SQL Server Client Access Licenses)
 - c. Click “Continue”
29. Then the SQL Server 2000 installation should start (it can take about 5-10 minutes)
30. Once the “Setup Complete” screen appears, click “Finish” to complete the installation



Installing Microsoft SQL Server 2000 SP3a Patch

1. The Microsoft SQL Server 2000 SP3a patch is included on the EPO CD.
2. Click on “Start” and then click on “Run”
3. In the “Open” field, enter “D:\sql2ksp3\setup.bat
4. Once the “Welcome” screen shows, click “Next”
5. At the “Software License Agreement”, click “Yes”
6. At the “Instance Name”, click “Next”
7. At the “Connect to Server” screen, do the following:
 - a. Click on “The SQL Server system administrator login information (SQL Server authentication)”
 - b. Under “Enter sa password”, enter the password for the **sa** account (you entered this during the SQL Server installation)
 - c. Click “Next”
8. At the “SQL Server 2000 Service Pack 3 Setup” screen, check “Upgrade Microsoft Search and apply SQL Server 2000 SP3 (required)”
9. Click “Continue”
10. At the “Error reporting” screen, click “OK”
11. At the “Start Copying Files” screen, click “Next”
12. Then it will start installing the SP3a files.
13. Near the end, a screen will pop-up stating “You should now backup your master and msdb databases

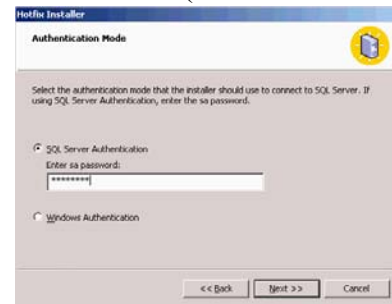


- since this installation has updated their content.” Click “OK” at this screen.
- At the “Setup Complete” screen, click “Finish”

Installing Microsoft SQL Server 2000 with SP3a Hotfixes

Installing MS03-031 Hotfix

- Click on “Start” and then click on “Run”
- In the “Open” field, enter “D:\SQL-Hotfixes\” and click “OK”
- Double click on the “MS03-031” folder
- Double click on the “SQL2000-KB815495-8.00.0818-ENU.exe” file
- At the “Welcome” screen, click “Next”
- At the “End User License Agreement” screen, do the following:
 - Check “I accept the licensing terms and conditions”
 - Click “Next”
- At the “Instance to Update” screen, accept the default instance (it should be the EPO/SUS Server name) and click “Next”
- At the “Authentication Mode” screen, do the following:
 - Click on SQL Server Authentication
 - Under “Enter sa password:”, enter the password for the sa account you set during the installation of SQL Server 2000
 - Click “Next”
- At the “Ready to Install” screen, click on “Install”
- It should start installing the patch
- At the “Hotfix Complete” screen, click “Finish”



Installing KB826161 Hotfix

- Click on “Start” and then click on “Run”
- In the “Open” field, enter “D:\SQL-Hotfixes\” and click “OK”
- Double click on the “KB826161” folder
- Double click on the “SQL2000Tools-KB826161-8.00.0819-ENU.exe” file
- At the “Welcome” screen, click “Next”
- At the “End User License Agreement” screen, do the following:
 - Check “I accept the licensing terms and conditions”
 - Click “Next”
- At the “Ready to Install” screen, click on “Install”
- It should start installing the patch
- At the “Hotfix Complete” screen, click “Finish”
- It is recommended that you reboot the server once this installation has completed.

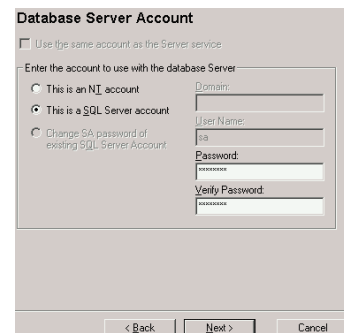
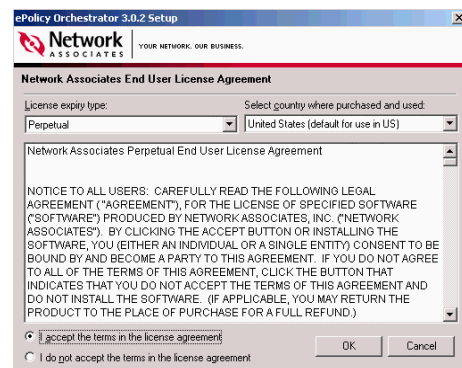
Installation of ePolicy Orchestrator 3.0.2a

Following steps should be run through on the ePO server:

Installation of ePO on the Server

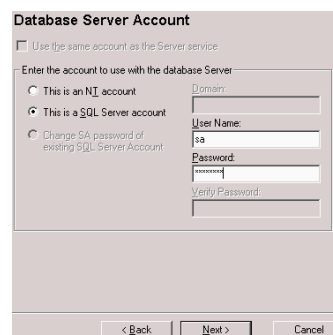
Installing ePO v3.0.1

1. Take the EPO Deployment CD and place it in the CD-ROM drive of the EPO/SUS server
2. Login to the EPO/SUS Server as an Administrator (**Note: the installation of EPO must be at the server console and not through a Remote Desktop or Terminal Services connection**)
3. Click on “Start” and then click on “Run”
4. In the Open box, type in “D:\EPO301\” and then click “OK” (D:\ being the drive letter of the server’s CD-ROM drive)
5. Double-click “setup.exe”
6. At the “ePolicy Orchestrator 3.01 Setup” screen, click “Next”
7. Under the “License expiry type”, choose “Perpetual”
8. In the same window, click on the “I Accept the terms in the license agreement”
9. Click the “OK” button
10. On the “Installation Options” screen, accept the defaults and click “Next”
11. On the “Server Service Account” screen, check “Use Local System Account” and click “Next”
12. A window will pop up stating, “This account is not a domain administrator. You may not be able to push the ePolicy Orchestrator Agent.”
13. Click the “OK” button
14. If you do NOT need Microsoft SQL Server 2000 loaded, do the following:
 - a. On the “Select Database Server” screen, select “Install a server on this computer and use it”
 - b. Click “Next”
 - c. On the “Database Server Account” screen, click on “This is a SQL Server account”
 - d. In the same window, enter and confirm the password (this will be the password for the local EPO Database, the username will be “sa”)
 - e. Click “Next”



15. If you do need Microsoft SQL Server 2000 loaded, make sure you have installed Microsoft SQL Server using the installation steps on page 7 through 9 and do the following:

- a. On the “Select Database Server” screen, select “Use the existing server on this computer”
- b. Click “Next”
- c. On the “Database Server Account” screen, click on “This is a SQL Server account”
- d. In the “User Name” field, enter “sa”
- e. In the “Password” field, enter the password for the sa account that you set in the SQL Server 2000 installation.
- f. Click “Next”



16. On the HTTP Configuration Screen, set the following:
 - a. HTTP port for Agent communication - 11500
 - b. HTTP port for Console communication - 11501
 - c. HTTP port for Agent Wake-Up communication - 11502
 - d. HTTP port for Agent Broadcast communication – 11503
17. Click “Next”
18. At the “Ready to Install” screen, click the “Install” button
19. During the “Executing Setup” screen, the ePO setup application is installing the necessary program files
20. In the middle of the installation, a screen will pop up stating “ePolicy Orchestrator 3.0.1 Setup will now reboot your system”
21. Click “OK” to reboot your server
22. Once it finishes rebooting, log into the server and you may get a message stating that the installation of ePO was interrupted. Click “OK” to continue the installation
23. When the installation is finished, the “Installation Complete” window will pop-up
24. Click “Finish” to complete the installation

Updating ePO v3.0.1 to ePO 3.0.2a

1. Make sure the EPO Deployment CD is in the CD-ROM drive of the EPO/SUS server
2. If not already logged in, login to the EPO/SUS Server as an Administrator (**Note: this update of EPO must be at the server console and not through a Remote Desktop or Terminal Services connection**)
3. Click on “Start” and then click on “Run”
4. In the Open box, type in “D:\EPO302a\” and then click “OK” (D:\ being the drive letter of the server’s CD-ROM drive)
5. Double-click “setup.exe” in the installation directory
6. If your video display is not set to 1024x768 or higher, then you will get an error message
7. Click “OK” if you get this message
8. When the “ePolicy Orchestrator 3.0.2 Setup” screen pops up, click “Next”

9. Under the “License Expiry Type”, choose “Perpetual”
10. In the same window, click on the “I Accept the terms in the license agreement”
11. Click “OK”
12. At the “Ready to Install” screen, click the “Install” button
13. An “Executing Setup” screen will pop up and show the progress of the installation
14. Once it finishes, the “Installation Complete” screen will show
15. Click “Finish”

Updating ePO to Patch 6

1. Make sure the EPO Deployment CD is in the CD-ROM drive of the EPO/SUS server
2. If not already logged in, login to the EPO/SUS Server as an Administrator (**Note: this update of EPO must be at the server console and not through a Remote Desktop or Terminal Services connection**)
3. Click on “Start” and then click on “Run”
4. In the Open box, type in “D:\EPO-Patch6\” and then click “OK” (D:\ being the drive letter of the server’s CD-ROM drive)
5. Double-click “setup.exe”
6. At the “ePolicy Orchestrator 3.0.2 PATCH 6 Setup” screen, click “Next”
7. Under the “License Expiry Type”, choose “Perpetual”
8. In the same window, click on the “I Accept the terms in the license agreement”
9. Click “OK”
10. At the “Ready to Install” screen, click the “Install” button
11. An “Executing Setup” screen will pop up and show the progress of the installation
12. Once it finishes, the “Installation Complete” screen will show
13. Click “Finish”
14. Reboot the EPO/SUS server (it should prompt you to do this)

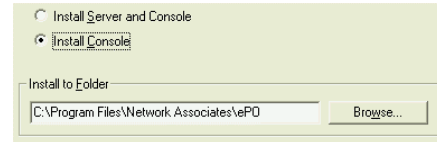
Installing ePO Remote Management Console on a Workstation

The following steps should be followed on the Windows XP with SP1 system you wish to manage ePO from:

Installing the ePO Management Console v3.0.1

1. Find a Windows XP workstation with Internet Explorer 6.0 or higher installed, 200MB of free hard drive space, and 256MB of RAM
2. Place the EPO Deployment CD in the CD-ROM drive of the workstation
3. If not already logged in, login to the workstation as an Administrator
4. Click on “Start” and then click on “Run”
5. In the Open box, type in “D:\EPO301\” and then click “OK” (D:\ being the drive letter of the workstation’s CD-ROM drive)
6. Double-click on “setup.exe”
7. On the “ePolicy Orchestrator 3.0.1 Setup” screen, click “Next”

8. When the “Network Associates End User License Agreement” screen appears, choose “Perpetual”, click “I accept the terms in the license agreement”, and click “OK”
9. At the “Installation Options” screen, click “Install Console”
10. Under “Install to Folder” accept the default
11. Click “Next”
12. When the “Ready to Install” screen appears, click “Install”
13. Once it has completed the installation, click “Finish”



Updating the ePO v3.0.1 Management Console to the ePO 3.0.2a Management Console

1. Make sure the EPO Deployment CD is in the CD-ROM drive of the workstation
2. If not already logged in, login to the workstation as an Administrator
3. In the Open box, type in “D:\EPO302a\” and then click “OK” (D:\ being the drive letter of the workstation’s CD-ROM drive)
4. Double-click “setup.exe”
5. On the “ePolicy Orchestrator 3.0.2 Setup” screen, click “Next”
6. When the “Network Associates End User License Agreement” screen appears, choose “Perpetual”, click “I accept the terms in the license agreement”, and click “OK”
7. When the “Ready to Install” screen appears, click “Install”
8. Once it has completed the installation, click “Finish”



Updating ePO to Patch 6

1. Make sure the EPO Deployment CD is in the CD-ROM drive of the workstation
2. If not already logged in, login to the workstation as an Administrator
3. In the Open box, type in “D:\EPO-Patch6\” and then click “OK” (D:\ being the drive letter of the workstation’s CD-ROM drive)
4. Double-click “setup.exe”
5. At the “ePolicy Orchestrator 3.0.2 Patch 6 Setup” screen, click “Next”
6. Under the “License Expiry Type”, choose “Perpetual”
7. In the same window, click on the “I Accept the terms in the license agreement”
8. Click “OK”
9. At the “Ready to Install” screen, click the “Install” button
10. An “Executing Setup” screen will pop up and show the progress of the installation
11. Once it finishes, the “Installation Complete” screen will show
12. Click “Finish”

Configuration of ePO Server

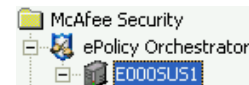
Pre-Configuration Tasks

Starting ePO for the First Time

1. Go to the workstation you installed the ePO Management Console on
2. Start ePolicy Orchestrator by going to Start -> Programs -> Network Associates -> ePolicy Orchestrator 3.0.2 Console
3. Once the ePolicy Orchestrator window pops up, click on the “Add Server” button 
4. A login screen should pop up, make sure that the following is entered
Server name: *Name of the server ePolicy Orchestrator is running on*
 - a. User name: admin
 - b. Password: admin
 - c. HTTP Port: 11501
5. Click “OK” to login
6. When the window on the right pops up, click “OK” 
7. The next window should force you to change the admin password. Enter an appropriate password for the admin account (we recommend making it the same password as the Local Administrator of the server you have ePO installed on)
8. You may get a window stating “Error accessing license information” just click “OK” if it pops up
9. At the ePolicy Orchestrator Login screen, change the password to the new password you just entered and click “OK”
10. The “Initializing” window will appear and start your first ePO session
11. You should have the following tabs at the top
 - a. General
 - b. Scheduled Tasks
 - c. Task Logs
 - d. Settings
 - e. Users

Creating a Global Administrator user for OET

1. Click on the server name in the left side of the ePO window
2. In the right window, click on the “Users” tab on the far right
3. Click the “Create User” button
4. In the “Name” field, enter **_EPOADMIN**
5. In the “Role” field, choose “Administrator”
6. In the “Password” field, enter **P@ssw0rd**
7. Click in the “Confirm Password” field and enter the same password
8. Then click the “Save” button at the top of the window



Installing EPO Agent Patch 7

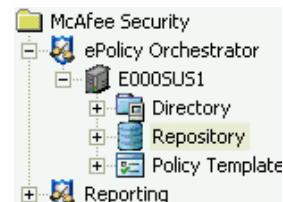
1. Make sure the EPO Deployment CD is in the CD-ROM drive of the workstation
2. If not already logged in, login to the workstation as an Administrator
3. Under the “C:\” drive, create a folder named “EPO”
4. Copy the “D:\Agent-Patch7” folder to the “C:\EPO” folder (D:\ being the workstation’s CD-ROM drive)
5. Open the EPO Remote Management Console and login to the EPO/SUS Server
6. In the directory on the left side of the window, click on “Repository”
7. In the “Repository” window on the right, click on “Check in a Package”
8. This will start the “Check in Package Wizard”, click “Next”
9. On the next window, click on “Products or Updates”, click “Next”
10. Then it will ask for the location of the “NAI Package Description File”, click on “Browse”
11. Go to “C:\EPO\Agent-Patch7\”
12. Click on the file named “PkgCatalog.z” or “PkgCatalog”, and then click “Open”
13. Click “Next”
14. It will then verify the package you specified
15. Once it finishes verifying, click “Finish”
16. It will start adding the EPO Agent Update package to the server
17. Once it finishes adding the package (it will say “Package checked in successfully.”), click “Close”
18. Copy the “C:\EPO\Agent-Patch7” folder from the workstation to [\\<EPO-Server-Name>\c\\$\EPO\](#) directory
19. Reboot the EPO Server



Configuring the Repository

Adding the VirusScan Enterprise v7.1 Program Files

1. Place the EPO CD-ROM in the CD drive of the EPO Remote Management workstation
2. Copy the VirusScan71 directory on the CD-ROM to the C:\ drive on the workstation (when completed, there should be a C:\VirusScan71 directory)
3. Logon to the EPO Remote Management Console
4. In the directory on the left side of the window, click on “Repository”
5. In the “Repository” window on the right, click on “Check in a Package”
6. This will start the “Check in Package Wizard”, click “Next”
7. On the next window, click on “Products or Updates”, click “Next”



8. Then it will ask for the location of the “NAI Package Description File”, click on “Browse”
9. Go to “C:\VirusScan71\”
10. Click on the file named “PkgCatalog.z” or “PkgCatalog”, and then click “Open”
11. Click “Next”
12. It will then verify the package you specified
13. Once it finishes verifying, click “Finish”
14. It will start adding the VirusScan v7.1 package to the server
15. Once it finishes adding the package, click “Close”
16. Click “Check in NAP”
17. In the “Software Repository Configuration Wizard”, click “Add New Software to Be Managed”
18. Click “Next”
19. At the “Select a Software Package” window, go to “C:\VirusScan71\” and choose the “VSE710.NAP” file
20. Click “Open”
21. It should check in the software and complete automatically

Adding the VirusScan v4.51 Program Files

1. Place the EPO CD-ROM in the CD drive of the EPO Remote Management workstation
2. Copy the VirusScan451 directory on the CD-ROM to the C:\ drive on the workstation (when completed, there should be a C:\VirusScan451 directory)
3. Logon to the EPO Remote Management Console
4. In the directory on the left side of the window, click on “Repository”
5. In the “Repository” window, click on “Check in a Package”
6. This will start the “Check in Package Wizard”, click “Next”
7. On the next window, click on “Products or Updates”, click “Next”
8. Then it will ask for the location of the “NAI Package Description File”, click on “Browse”
9. Go to “C:\VirusScan451\”
10. Click on the file named “PkgCatalog.z” or “PkgCatalog”, and click “Open”
11. Click “Next”
12. It will then verify the package you specified
13. Once it finishes verifying, click “Finish”
14. It will start adding the VirusScan v4.51 package to the server
15. Once it finishes adding the package, click “Close”
16. Click “Check in NAP”
17. In the “Configure Software Repository” window, click “Add New Software to Be Managed”
18. Click “Next”
19. At the “Select Software Package” window, go to “C:\VirusScan451” and select “VSC451A.NAP” file
20. Click “Open”

21. If you get a dialog which states “Software package already installed. Do you want to overwrite?”, click “Yes”.
22. It should check in the software and complete automatically

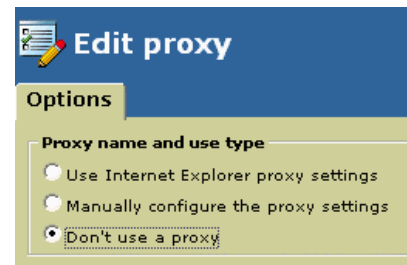
Installing the CorrectENG.EXE update

(Fixes a potential issue with VirusScan 7.1 updating its engine from EPO)

1. Open the ePO Remote Console on your workstation and login to your server
2. In the directory on the left side of the window, click on “Repository”
3. In the “Repository” window on the right, click on “Check in a Package”
4. This will start the “Check in Package Wizard”, click “Next”
5. On the next window, click on “SuperDAT”, click “Next”
6. Then it will ask for the location of the “NAI Package Description File”, click on “Browse”
7. Go to “D:\CorrectENG\” and click on “CorrectENG.EXE” (D:\ being the CD drive of the workstation)
8. Click “Open”
9. Click “Next”
10. It will verify the package quickly, then click “Next”
11. Select “Current”, check “Support legacy product update”, check “Move existing package to the ‘Previous’ branch”, and click “Finish”
12. Click “Close”

Configuring Proxy Settings for Pulling DAT Updates from NAI

1. Open the ePO Remote Console on your workstation and login to your server
2. In the directory on the left side of the window, click on “Repository”
3. In the “Repository” window on the right, click on “Configure proxy settings” (it is at the bottom of the list)
4. At the “Edit proxy” screen, click on “Don’t use a proxy”
5. Click “OK” to save settings and close the window



Creating Task to Pull DAT Updates from NAI

1. In the left section, click on “Repository”
2. In the “Repository” window, on the list at the left, click on “Schedule Pull Tasks”
3. In the “Scheduled Tasks” tab, click “Create Task”
4. In the “Configure New Task” window, under “Task Settings” enter the following:
 - a. Name: Daily DAT Pull from NAI
 - b. Task Type: Repository Pull
 - c. Enable Task: Yes
 - d. Schedule Type: Daily
 - e. In the “Daily” section, enter “Every 1 days”
5. Click on “Advanced schedule options” to expand it

6. Under “Advanced schedule options”, enter the following:
 - a. Start Time: 7:00pm
 - b. Start Date: Current date
 - c. Do NOT check “End Date”
 - d. Check “Repeat Task”
 - e. For “Every”, enter “4”, and select “hours” from the drop down menu
 - f. Then set the “Duration” to “23 hours” and “59 minutes”
7. Under Additional Settings enter
 - a. Randomize Execution Time: No
 - b. Run Missed Task: No
 - c. Stop task if execution time exceeds limit: No
8. Click “Next” at the top
9. In the “Repository Pull Task” section, set the following:
 - a. Source Repository: NAIFtp
 - b. Destination Branch: Current
 - c. Support legacy product update: Checked
 - d. Move existing packages to the ‘previous’ branch: Unchecked
10. Click “Finish” at the top
11. Click “OK” at the window stating “Task has been scheduled”
12. You should see your new task in the “Scheduled Tasks” list

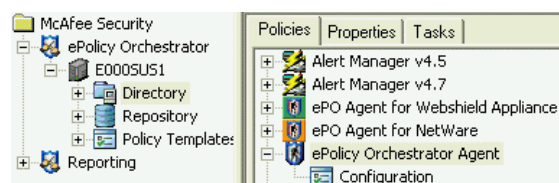
Manually Pulling the DAT File from NAI

1. Click on “Repository”
2. Click on “Pull Now”
3. In the “Pull Now Wizard”, click “Next”
4. Select “NAIFtp” and click “Next”
5. Select “Current”, check “Support legacy product update”, check “Move existing package to the ‘Previous’ branch”, and click “Finish”
6. The ePO server will download the newest DAT files available for your products
7. When finished, it will say “Pull successful”, click “Close”

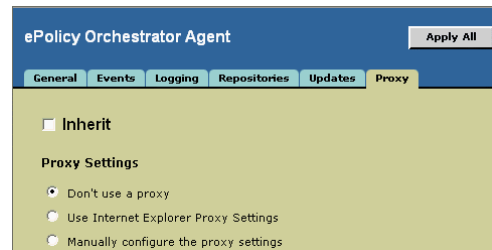
Setting Program Policies

ePolicy Orchestrator Agent Configuration

1. In the left section, click “Directory” and make sure, in the right window, that the “Policies” tab is selected
2. In the “Policies” list, double-click on “ePolicy Orchestrator Agent”



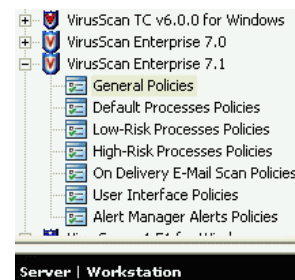
3. Double-click on “Configuration” below the “ePolicy Orchestrator Agent”
4. Under the “General” tab, uncheck the box beside “Inherit”
5. Under “General Options”
 - a. Show Agent tray icon: unchecked
 - b. Enable Agent wakeup call support: checked
 - c. Enable agent Upgrade from 2.x Agent to 3.0 Agent: unchecked
 - d. Policy enforcement interval: 60 minutes
6. Under “Software Installation”, accept the default settings
7. Under “Agent Communication Intervals”, enter the following:
 - a. Enable Agent to Server communication: Checked
 - b. Agent to Server communication interval: 240 minutes
 - c. Policy age to trigger 10 minute communication interval: 1 days
 - d. On each agent to server communication interval, set the following properties: Full Properties
8. Scroll up the frame and click on Repositories tab (it is at the top of the frame)
9. Uncheck “Inherit”
10. Set to following:
 - a. Under “Inherit” select “Use ePO configured repositories”
 - b. Under “Repository” selection, select “Ping time”
 - c. In the “Repository” list, make sure that “ePO_Servername” is checked and “NAIFtp” is unchecked
11. Scroll up the frame and click on the “Proxy” tab
12. Uncheck “Inherit”
13. Click on “Don’t use a proxy” (the remaining options below should gray out)
14. Click “Apply All” at the top right

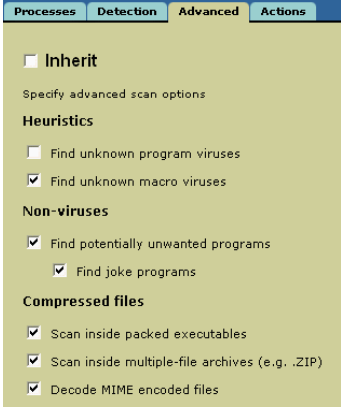
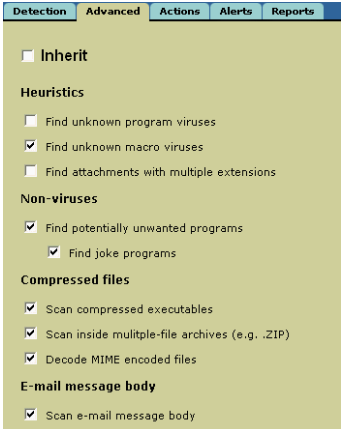


VirusScan Software

VirusScan Enterprise v7.1 Workstation settings


1. In the left section, click on “Directory” and then make sure in the right window that the “Policies” tab is selected
2. In the “Policies” list, double-click on “VirusScan Enterprise 7.1”
3. In the “VirusScan Enterprise 7.1” list, click “General Polices”
4. You should see a small arrow pointing to “Workstation”, this means you will be editing the Workstation settings for VirusScan v7.1
5. Under the “General Tab”, do the following:
 - a. Uncheck “Inherit”
 - b. Boot Sector(s): Check
 - c. Floppy during shutdown: Unchecked



- d. Enable on-access scanning at system startup: Checked
 - e. Enable on-access scanning when the policy is enforced. (Deselect this option to disable on-access scanning when the policy is enforced.): Checked
 - f. Quarantine folder: “\quarantine”
 - g. Maximum archive scan time (seconds): 15
 - h. Enforce a maximum scanning time for all files: Checked
 - i. Maximum scan time (seconds): 45
 - j. Click “Apply”
6. For the “Messages” and “Reports” tabs, accept the defaults
 7. Click on “Default Processes Policies” under “VirusScan Enterprise 7.1”
 8. Under the “Advanced” tab, do the following:
 - a. Uncheck “Inherit”
 - b. Find unknown program viruses: Unchecked
 - c. Find unknown Macro viruses: Checked
 - d. Find potentially unwanted programs: Checked
 - e. Find joke programs: Checked
 - f. Scan inside packed executables: Checked
 - g. Scan inside multiple-file archives (e.g. .ZIP): Checked
 - h. Decode MIME encoded files: Checked
 - i. Scroll up and click “Apply”
- 
9. Click on “On Delivery E-Mail Scan Policies” under “VirusScan Enterprise 7.1”
 10. Under the “Advanced” tab, do the following:
 - a. Uncheck “Inherit”
 - b. Find unknown program viruses: Unchecked
 - c. Find unknown Macro viruses: Checked
 - d. Find attachments with multiple extensions: Unchecked
 - e. Find potentially unwanted programs: Checked
 - f. Find joke programs: Checked
 - g. Scan inside packed executables: Checked
 - h. Scan inside multiple-file archives (e.g. .ZIP): Checked
 - i. Decode MIME encoded files: Checked
 - j. Scan e-mail message body: Checked
 - k. Scroll up and click “Apply”
- 
11. Click on “User Interface Policies” under “VirusScan Enterprise 7.1”
 12. Under the Display Options tab, do the following:
 - a. Uncheck “Inherit”
 - b. In the “System Tray Icon” section: select “Show the system tray icon with minimal menu options”
 - c. Refresh the VirusScan console screen every: 3 seconds

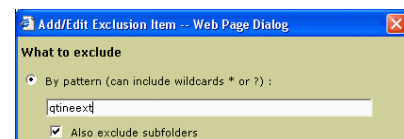
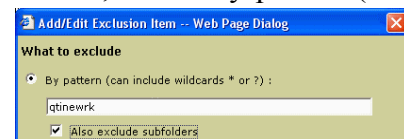
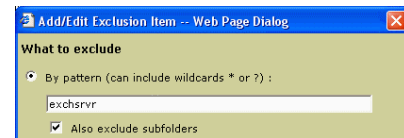
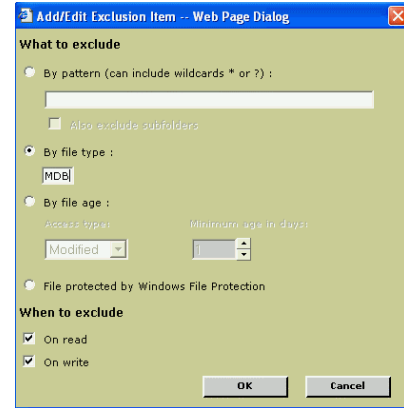
- d. Display ePO's tasks in the VirusScan console (requires ePO 3.0 or higher): Unchecked
 - e. Disable default AutoUpdate task schedule: Checked
 - f. Enable VirusScan splash screen: Checked
13. Under the "Password Options" tab, do the following:
- a. Uncheck "Inherit"
 - b. In the "User Interface Password" section, select "Password protection for all items listed below"
 - c. Then enter and confirm a password. Note: This will password protect VirusScan on workstations so that no settings can be changed or altered at the workstation unless they use that password
 - d. Click "Apply"

VirusScan Enterprise 7.1 Server Settings

1. In the left section, click on "Directory", then make sure in the right window that the "Policies" tab is selected
2. In the "Policies" list, double-click on "VirusScan Enterprise 7.1"
3. Under "VirusScan Enterprise 7.1" list, click on "General Policies"
4. At the top left of the "General Policies" window, click "Server" 
5. Under the "General Tab", do the following:
 - a. Uncheck "Inherit"
 - b. Boot Sector(s): Check
 - c. Floppy during shutdown: Unchecked
 - d. Enable on-access scanning at system startup: Checked
 - e. Enable on-access scanning when the policy is enforced. (Deselect this option to disable on-access scanning when the policy is enforced.): Checked
 - f. Quarantine folder: "\\quarantine"
 - g. Maximum archive scan time (seconds): 15
 - h. Enforce a maximum scanning time for all files: Checked
 - i. Maximum scan time (seconds): 45
 - j. Click "Apply"
6. For the "Messages" and "Reports" tabs, accept the defaults
7. Then click on "Default Processes Policies" under "VirusScan Enterprise 7.1"
8. At the top left of the "Default Processes Policies" window, click on "Server"
9. Under the "Detection" tab, do the following:
 - a. Uncheck "Inherit"
 - b. Scan Files Section
 - i. When writing to disk: Checked
 - ii. When reading from disk: Checked
 - iii. On network drives: Unchecked
 - c. What to scan
 - i. All files: Selected

d. What not to scan

- i. Overwrite client exclusions:
Unchecked
- ii. Click on the “Exclusions” button
- iii. In the “Set Exclusions” window, click “Add”
- iv. In the “Add/Edit Exclusion Item” window, click “By File Type”
- v. In the field enter “MDB”
- vi. In the “When to Exclude” section, make sure “On Read” and “On Write” are checked
- vii. Click “OK”
- viii. Repeat these steps for the following file types
 1. EDB
 2. MDF
 3. LDF
 4. TPS (for STI Servers)
- ix. In the “Set Exclusions” window, click “Add”
- x. In the “Add/Edit Exclusion Item” window, click “By pattern (can include wildcards * or ?) :”
- xi. In the field enter “**exchsrvr**”
- xii. Check “Also exclude subfolders”
- xiii. In the “When to Exclude” section, make sure “On Read” and “On Write” are checked
- xiv. Click “OK”
- xv. In the “Set Exclusions” window, click “Add”
- xvi. In the “Add/Edit Exclusion Item” window, click “By pattern (can include wildcards * or ?) :”
- xvii. In the field enter “**qtnewrk**”
- xviii. Check “Also exclude subfolders”
- xix. In the “When to Exclude” section, make sure “On Read” and “On Write” are checked
- xx. Click “OK”
- xxi. In the “Set Exclusions” window, click “Add”
- xxii. In the “Add/Edit Exclusion Item” window, click “By pattern (can include wildcards * or ?) :”
- xxiii. In the field enter “**qtineext**”
- xxiv. Check “Also exclude subfolders”
- xxv. In the “When to Exclude” section, make sure “On Read” and “On Write” are checked
- xxvi. Click “OK”
- xxvii. In the “Set Exclusions” window, click “OK”



10. Scroll up the frame and click on the “Advanced” tab

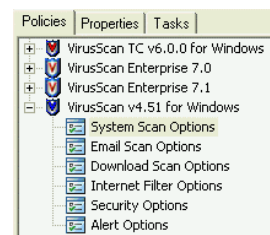
11. Under the “Advanced” tab, do the following:

- a. Uncheck “Inherit”

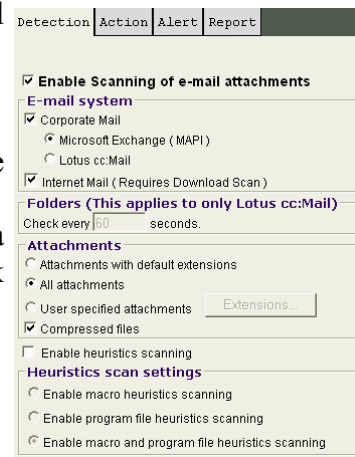
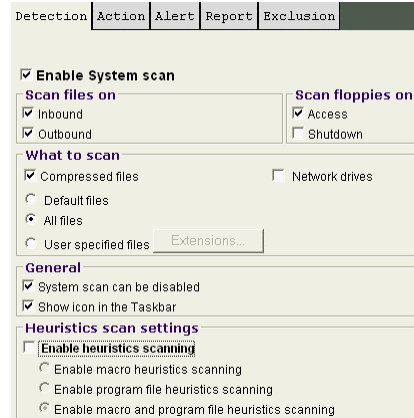
- b. Find unknown program viruses: Unchecked
 - c. Find unknown Macro viruses: Checked
 - d. Find potentially unwanted programs: Unchecked
 - e. Find joke programs: Unchecked
 - f. Scan inside packed executables: Checked
 - g. Scan inside multiple-file archives (e.g. .ZIP): Checked
 - h. Decode MIME encoded files: Checked
12. Scroll up and click “Apply”
13. Click on “On Delivery E-Mail Scan Policies” under “VirusScan Enterprise 7.1”
14. At the top left of the “On Delivery E-Mail Scan Policies” window, click “Server”
15. Under the “Detection” tab, do the following:
- a. Uncheck “Inherit”
 - b. Enable Microsoft Exchange (MAPI, IMAP): Unchecked
 - c. Under “Scanning of attachments”: All file types is selected
16. Click “Apply”
17. Click on “User Interface Policies” under “VirusScan Enterprise 7.1”
18. At the top left of the “User interface Policies” window, click “Server”
19. Under the “Display Options” tab, do the following:
- a. Uncheck “Inherit”
 - b. In the “System Tray Icon” section: select “Show the system tray icon with all menu options” (default setting)
 - c. Refresh the VirusScan console screen every: 3 seconds
 - d. Display ePO’s tasks in the VirusScan console (requires ePO 3.0 or higher): Unchecked
 - e. Disable default AutoUpdate task schedule: Checked
 - f. Enable VirusScan splash screen: Checked
20. Under the “Password Options” tab, do the following:
- e. Uncheck “Inherit”
 - f. In the “User Interface Password” section, select “Password protection for all items listed below”
 - g. Then enter and confirm a password. Note: This will password protect VirusScan on servers so that no settings can be changed or altered at the server unless they use that password
14. Click “Apply”

VirusScan 4.5.1 Settings

1. In the left section, click on “Directory” and make sure in the right window that the “Policies” tab is selected
2. In the “Policies” list, double-click on “VirusScan v4.51 for Windows”
3. Under “VirusScan v4.51 for Windows”, click on “System Scan Options”
4. Under the “Detection” tab, do the following:
 - a. Uncheck “Inherit” (it is at the top right)



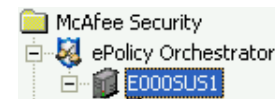
- b. In the “Scan Floppies On” section, uncheck “Shutdown”
 - c. In the “What To Scan” section, select “All Files”
 - d. In the “General” section, uncheck “System scan can be disabled”
 - e. At the bottom right, click “Apply”
5. Under the “Action” tab, do the following:
 - a. Uncheck “Inherit”
 - b. At the bottom of the window, select “Clean infected files automatically”
 - c. Scroll down and click “Apply”
6. Under “VirusScan v4.51 for Windows”, click “Email Scan Options”
 - a. Under the “Detection” tab, do the following:
 - i. Uncheck “Inherit”
 - ii. Check “Enable Scanning of e-mail attachments”
 - iii. Under “E-mail System”
 1. Check “Corporate Mail”
 2. Select “Microsoft Exchange (MAPI)”
 3. Check “Internet Mail” – a window will pop-up, click “OK”
 - iv. Under the “Attachments” section
 1. Select “All Attachments”
 2. Check “Compressed Files”
 - v. Click “Apply”
7. Under “VirusScan v4.51 for Windows”, click on “Download Scan Options”
 - a. Under the “Detection” tab, do the following:
 - i. Uncheck “Inherit”
 - ii. Under the “What to Scan” section
 1. Select “All Files”
 2. Check “Scan Compressed Files”
 - iii. Scroll down and click “Apply”
 - b. Scroll up and under the “Action” tab, do the following:
 - i. Uncheck “Inherit”
 - ii. Under the “When a Virus” is Found section
 1. Select “Delete infected files automatically”
 - iii. Scroll down and click “Apply”
8. Under “VirusScan v4.51 for Windows”, click on “Internet Filter Options”
 - a. Under the “Detection” tab, do the following:
 - i. Uncheck “Inherit”
 - ii. Check “Enable Java and ActiveX Scanning”
 - iii. Accept the defaults for the remaining choices
 - iv. Scroll down and click “Apply”



9. Under “VirusScan v4.51 for Windows”, click on “Security Options”
 - a. Under the “Password” tab, do the following:
 - i. Uncheck “Inherit”
 - ii. Check “Enable password protection for all property pages”
 - iii. Under “Pages to Password Protect” section, select “Password-protect all options on all property pages”
 - iv. Under the “Password” section, enter a password needed to change VirusScan settings on workstations (We recommend that you use the same password that you assigned to VirusScan 7.1)
 - v. Click “Apply”

Creating Agent Installation Package

1. Click on the server name on the left hand side of the window
2. Under the “General” tab, click on “Agent Installation Package Creation Wizard”
3. At the “Agent Installation Package Creation Wizard” window, click “Next”
4. It will ask for “User Credentials”, enter “<DISTRICT DOMAIN>_EPOAdmin”
5. Then enter and confirm the password for _EPOAdmin
6. Click “Next”
7. Then it should ask you for an “Installation Directory”, click “Browse”
8. Go to [\\<EPO/SUS-Server\EPO-Agent\](#) and click “OK”
9. Click “Next”
10. At the “Create Package” window, click “Next”
11. Click “Finish”



Setting up the Directory

Note: To help you with this section, an Excel spreadsheet named “EPO IP Calculator” has been created to do a lot of the calculations for you. You will need to have the IP Address of your Domain Controller to calculate its network and the Gateway/Router IP Address for the remaining networks. This spreadsheet should be located in the root of “D:\” (D:\ being the CD-ROM drive)

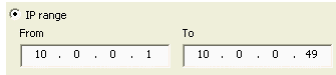
Adding the District Site

1. In the left side, you will see a directory structure with your server listed and under it “Directory”, “Repository”, and “Policy Templates”
2. Right click on “Directory”, go down to “New”, and then select “Site”
3. On the “Add Sites” screen, click “Add”
4. On the “New Site” screen, in the “Name” field, enter the district name
5. Under “Type”, do NOT check “Domain. Leave it unchecked.
6. Click the “Add” button at the bottom in the “IP Management” section
7. Click on “IP Range “

8. Find the IP Range that the Domain Controller's IP Address is in
9. For the "From" part of the IP Range enter the first 3 numbers of the Domain Controller's IP address and then "1" for the last number (for example, if the Domain Controller's address is 10.x.x.50, you would enter 10.x.x.1)
10. For the "To" part of the IP Range, enter the first 3 numbers of the Domain Controller's IP address and then "49" for the last number
11. Click on "OK"
12. Click the "Add" button at the bottom in the "IP Management" section
13. Click on "IP Range"
14. For the "From" part of the IP Range enter the first 3 numbers of the Domain Controller's IP address and then "60" for the last number (for example, if the Domain Controller's address is 10.x.x.50, you would enter 10.x.x.60)
15. For the "To" part of the IP Range, enter the first 2 numbers of the Domain Controller's IP address, add 15 to the third number and enter that number, and then "254" for the last number. (for example, if the Domain Controller's address is 10.x.0.50, you would enter 10.x.15.254)
16. Click on "OK"
17. You next want to get a list of IP networks for your district
 - a. Get or make a list of an IP address from each network in your district.
 - b. For each network's IP address, write down the first three numbers (starting from the left). For example, for 10.x.16.1 you would write down 10.x.16
 - c. Then add a "0" as the last number. It should look like 10.x.16.0
 - d. The number you have for each network is the network name and will be used to set the "IP subnet mask" in ePO
18. Click the "Add" button at the bottom in the "IP Management" section
19. Click on "IP subnet mask"
20. Under "IP subnet mask", enter the network name (one of the numbers like 10.x.16.0 that you wrote down above) of one of your school district's networks
21. For the second number, you want to enter "20"
22. Click "OK"
23. Repeat steps 17-21 for all of your school district's networks except for the Domain Controller's range you entered in Steps 7-14
24. Click "OK" to finish

Adding the Server group

1. Right-click the District Site you created, select "New", then select "Group"
2. Click "Add"
3. In the "Name" field, enter "Servers"
4. For the main server range (the range where the Domain Controller is located),
 - a. Click the "Add" button at the bottom in the "IP Management" section

- b. Click on “IP Range”
 - c. For the “From” part of the IP Range, enter the first 3 numbers of the Domain Controller’s IP address and then “1” for the last number
 - d. For the “To” part of the IP Range, enter the first 3 numbers of the Domain Controller’s IP address and then “49” for the last number
- 
- e. Click on “OK”
 - f. Click the “Add” button at the bottom in the “IP Management” section
 - g. Click on “IP Range”
 - h. For the “From” part of the IP Range enter the first 3 numbers of the Domain Controller’s IP address and then “60” for the last number (for example, if the Domain Controller’s address is 10.x.x.52, you would enter 10.x.x.60)
 - i. For the “To” part of the IP Range enter the first 3 numbers of the Domain Controller’s IP address and then “254” for the last number (for example, if the Domain Controller’s address is 10.x.x.50 you would enter 10.x.x.254)
 - j. Click on “OK”
5. Take the remaining subnets you entered in the district site and do the following (These will be the subnet numbers that you entered in the “Adding the District Site” section):
 - a. Go to the “IP Management” section and click “Add”
 - b. Click on “IP Range”
 - c. In the “From” section, enter the first 3 numbers in the subnet (for example 10.1.16.0 would be 10.1.16)
 - d. For the fourth number enter “1” (i.e. 10.1.16.1)
 - e. In the “To” section, enter the same first 3 numbers in the subnet
 - f. For the fourth number enter “254” (i.e. 10.1.16.254)
 - g. Click “OK”
 - h. Repeat for the other subnets
 6. Once you are finished and are back to the “Add Groups” window, click “OK”

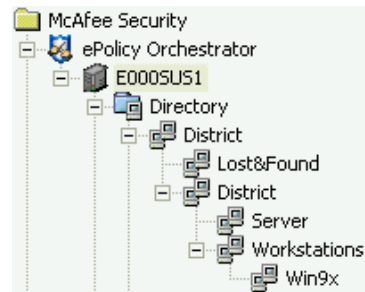
Adding the Workstations group

1. Right-click the District Site you created, select “New”, then select “Group”
2. Click “Add”
3. In the “Name” field, enter “Workstations”
4. For the main server range (the range where the Domain Controller is located),
 - a. Click the “Add” button at the bottom in the “IP Management” section
 - b. Click on “IP Range”
 - c. For the “From” part of the IP Range, enter the first 2 numbers of the Domain Controller’s IP address
 - d. For the third number, take the third number in the Domain Controller’s IP Address and add 1, then enter that number
 - e. For the fourth number, enter “1” (For example, if your DC’s IP Address is 10.x.0.50, then you would enter 10.x.1.1)

- f. For the “From” part of the IP Range, enter the first 2 numbers of the Domain Controller’s IP address
 - g. For the third number, take the third number in the Domain Controller’s IP Address and add 15, then enter that number
 - h. For the fourth number, enter “254” (For example, if your DC’s IP Address is 10.x.0.50, then you would enter 10.0.15.254)
5. For the subnets you entered in the district site, do the following (These will be the subnet numbers that you entered in the “Adding the District Site” section):
 - a. Go to the “IP Management” section and click “Add”
 - b. Click on “IP Range”
 - c. For the “From” part of the IP Range, enter the first 2 numbers in the subnet, add 1 to the third number and enter that number, and then enter “1” for the last number (if the subnet was 10.x.16.0, you would enter 10.1.17.1)
 - d. For the “To” part of the IP Range, enter the first 2 numbers in the subnet, add 15 to the third number and enter that number, and then “254” for the last number (if the subnet was 10.x.16.0, you would enter 10.x.31.254)
 - e. Click “OK”
 - f. Repeat for the remaining subnets
6. Once you are finished and are back to the “Add Groups” window, click “OK”

Adding the Win9x Group

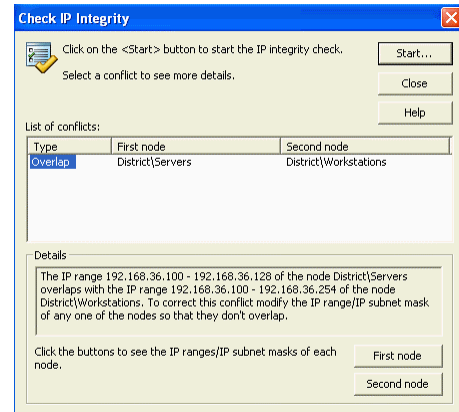
1. Right click on the “Workstations” group you created and choose “New”
2. Select “Group”
3. At the “Add Group” window, click “Add”
4. At the “New Group” window, in the “Name” field, enter “Win9x”
5. Click “OK”
6. At the “New Group” window, click “OK”



Testing Directory IP Configuration

1. The reason you need to do this is that EPO can sort using the IP Address of each machine. However, for this to work, the District Sites and Groups must be setup correctly. The District Site should cover all of the IP Addresses that you want ePolicy Orchestrator to manage (for our purposes, all except the Domain Controller range). The Servers and Workstations groups should have IP Ranges that are part of the District Site range. Errors can be caused if they are not entered correctly. This tool checks the District Site and Group settings to make sure that they will not cause any errors. We still recommend that you go back and double check the District Site and Groups so that all the correct IP Ranges and Subnets were entered for your district.
2. Right click on “Directory” and choose “All Tasks”
3. Select “IP Integrity Check” from the list

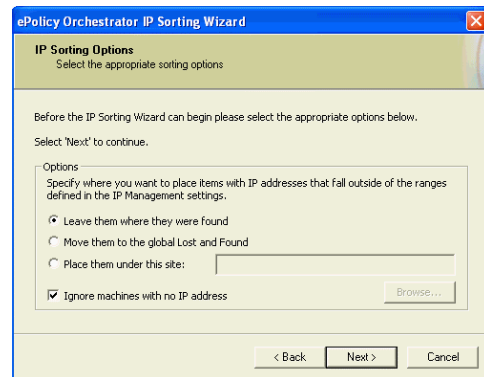
4. Click “Start” to check your setup
 - a. It will stop and show any IP conflicts there are between the District Site and Groups. To make changes to existing Sites and Groups, do the following:
 - i. Click on the District Site name under “Repository”
 - ii. Click on the “Properties” tab
 - iii. If you need to add an IP Range/Subnet, click on “Add...”
 - iv. Enter the IP Range/Subnet and click “OK”
 - v. Click “Apply” (changes will not take effect until you click Apply)
 - vi. If you need to edit an IP Range/Subnet, click on the Range/Subnet you want to change and then click “Edit...”
 - vii. Make any necessary changes, then click “OK”
 - viii. Click “Apply” (changes will not take effect until you click Apply)
 - b. If errors are found, you should see one of the following types of errors:
 - i. Site – A District Site has no IP Ranges or Subnets assigned to it, but it has a Group that has an IP Range assigned to it. Check the Site and make sure that the District Site has IP Ranges and Subnets assigned to it.
 - ii. Subnet – A group under the District Site has an IP Range that is outside the IP Ranges/Subnets of the District Site. Check the properties of both the Group and the District Site. Make sure that each range or subnet was entered correctly.
 - iii. Overlap – Two groups have IP Ranges that overlap. Check the properties of the Servers and Workstations groups and make sure that the IP Ranges were entered correct and make needed changes.
 - c. You can also check the “Details” section at the bottom to see specific information about the error.
5. Once you have made any necessary changes, run the “IP Integrity Check” again
6. When you get the message “No IP conflicts were found.”, click “OK”
7. Click “Close” to close the window



Sorting Computers by IP Address

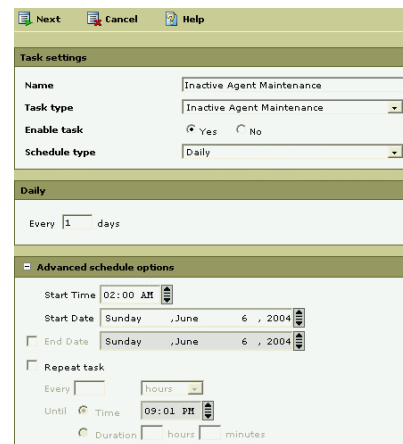
1. Right click on “Directory” and choose “All Tasks”

2. Select “Sort Computers by IP...” from the list
3. At the “IP Sorting Wizard” screen, click “Next”
4. At the “IP Sorting Options” screen, do the following (these are the defaults):
 - a. Select “Leave them where they were found”
 - b. Check “Ignore machines with no IP address”
5. Click “Next” (it will start sorting, it may take a little time depending upon the number of computers in the Directory)
6. Once it is finished sorting, click “Next”
7. Click “Finish”



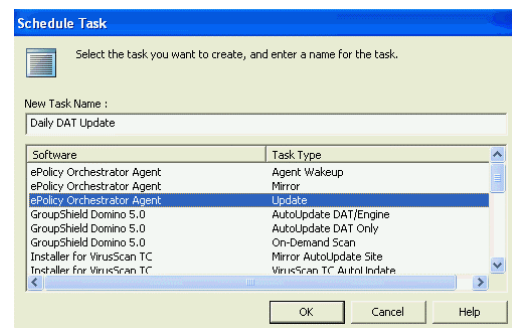
Inactive Agent Maintenance Task

1. Click on the server name in the list
2. In the right area, click on the “Scheduled Tasks” tab
3. Click on “Create Task”
4. For “Name”, enter “Inactive Agent Maintenance”
5. For “Task Type”, select “Inactive Agent Maintenance”
6. For “Enable Task”, click “Yes”
7. For “Schedule Type”, choose “Daily”
8. Under the “Daily” section, enter “Every 1 Days”
9. Double-click on “Advanced Schedule Options”
10. Enter “2:00 AM” in the “Start Time” field
11. At the top, click “Next”
12. For “Period of Inactivity”, enter “90 Days”
13. For “Action to Perform”, select “Delete”
14. Click “Finish”
15. A small window should pop up saying that the task has been scheduled
16. Click “OK”

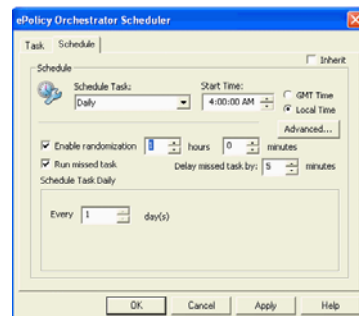
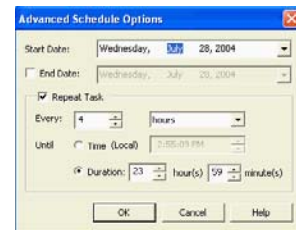
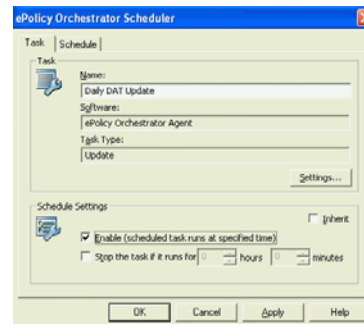


Setting Up the DAT File Update Task

1. Click on “Directory”
2. In the “Directory” window, click on the “Tasks” tab
3. Right click in the “Tasks” white area and select “Schedule Task”
4. In the “Schedule Task” window, under the “New Task Name” field, enter “Daily DAT Update”
5. In the list, click on “ePolicy Orchestrator Agent – Update”



6. Click “OK”
7. Double-click the “Daily DAT Update” task
8. In the “ePolicy Orchestrator Scheduler” window, under the “Schedule Settings” section, do the following:
 - a. Uncheck “Inherit”
 - b. Check “Enable”
9. Click on the “Schedule” tab, do the following:
 - a. Uncheck “Inherit”
 - b. Click on the “Advanced...” button
 - c. At the “Advanced Schedule Options” screen, check “Repeat Task”
 - d. Set “Every:”, enter “4 hours”
 - e. Under “Until”, click “Duration”
 - f. For “Duration”, enter “23 hours” and “59 minutes”
 - g. Click “OK”
 - h. Set “Schedule Task” to “Daily”
 - i. Set “Start Time” to “4:00 AM” and “Local Time”
 - j. Check “Enable randomization”
 - k. Set “Enable randomization” to “1 hour” and “0 minutes”
 - l. Check “Run Missed Task”
 - m. Set “Delay Missed Task By” to “5 minutes”
 - n. Set “Schedule Task Daily” for every “1 day(s)”
 - o. Click “OK”



Setting Up the Emergency DAT Update Task

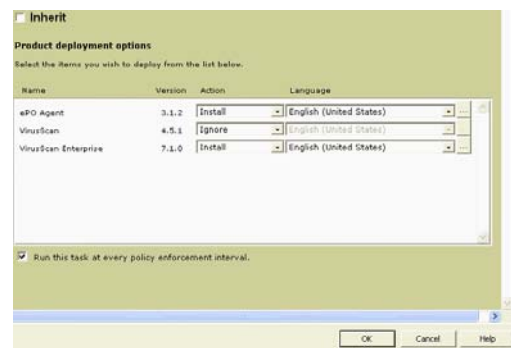
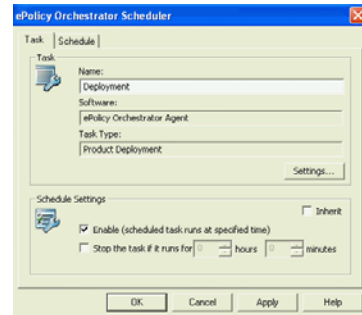
1. Click on “Directory”
2. In the “Directory” window, click on the “Tasks” tab
3. Right click in the “Tasks” white area and select “Schedule Task”
4. In the “Schedule Task” window, under the “New Task Name” field, enter “Emergency DAT Update”
5. In the list, click on “ePolicy Orchestrator Agent – Update”
6. Click “OK”
7. Double-click the “Emergency DAT Update” task
8. In the “ePolicy Orchestrator Scheduler” window, under the “Schedule Settings” section, do the following:
 - a. Uncheck “Inherit”
 - b. Leave “Enable” **unchecked**
9. Click on the “Schedule” tab, do the following:
 - a. Uncheck “Inherit”
 - b. Set “Schedule Task” to “Run Immediately”

- c. Check “Enable randomization”
- d. Set “Enable randomization” to “0 hour” and “10 minutes”
- e. Click “OK”

Setting up Installation Tasks

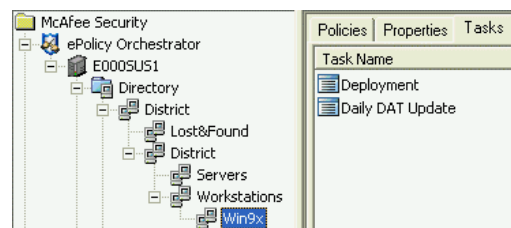
VirusScan v7.1 Installation (for Window NT 4.0, 2000, XP, and 2003 clients)

1. Click on “Directory”
2. Click on the “Tasks”
3. Double-click on “Deployment” in the “Task” list
4. At the “ePolicy Orchestrator Scheduler” screen, click on the “Task” tab
5. In the “ePolicy Orchestrator Scheduler” window, under the “Schedule Settings” section, do the following:
 - a. Uncheck “Inherit”
 - b. Check “Enable”
6. Click “Settings”
7. Uncheck “Inherit”
8. Next to “ePO Agent”, click “Ignore” and change it to “Install”
9. Make sure the Language it set for “English”
10. Next to “VirusScan Enterprise”, click “Ignore” and change it to “Install”
11. Make sure the Language it set for “English”
12. Click “OK”
13. At the “ePolicy Orchestrator Scheduler” screen, click on the “Schedule” tab
14. Uncheck “Inherit” at the top right
15. Change “Schedule Task” to “Run Immediately”
16. Then click “OK”



VirusScan v4.51 Installation (for Windows 95 and 98 clients)

1. Expand the “Directory”
2. Expand the District Site
3. Expand the “Workstations” group
4. Click the “Win9x” group
5. Click the “Tasks” tab
6. Double-click on “Deployment” in the “Task” list
7. At the “ePolicy Orchestrator Scheduler” screen, click on the “Task” tab



8. In the “ePolicy Orchestrator Scheduler” window, under the “Schedule Settings” section, do the following:

- a. Uncheck “Inherit”
- b. Check “Enable”

9. Click “Settings”

10. Uncheck “Inherit”

11. Next to “ePO Agent”, click “Ignore” and change it to “Install”

12. Make sure the Language is set for “English”

13. Next to “VirusScan”, click on “Ignore” and change it to “Install”

14. Make sure the “Language” is set for “English”

15. Change the setting next to “VirusScan Enterprise” from “Install” to “Ignore”

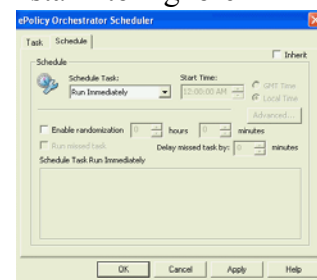
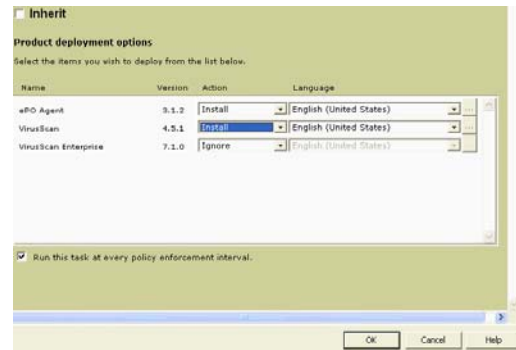
16. Click “OK” at the bottom

17. At the “ePolicy Orchestrator Scheduler” screen, click on the “Schedule” tab

10. Uncheck “Inherit” at the top right

11. Change “Schedule Task” to “Run Immediately”

12. Click “OK”



Installing the ePolicy Orchestrator Agent on Servers

Note: It is recommended that you manually install the EPO Agent on servers.

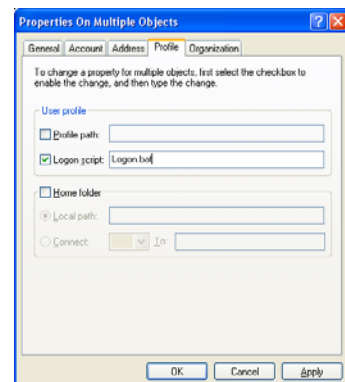
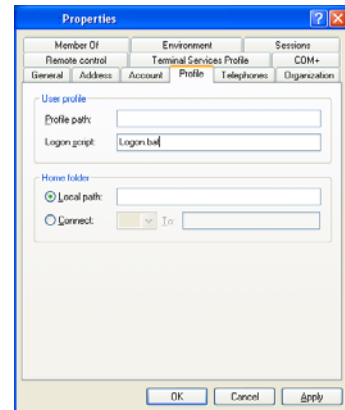
1. Logon as an Administrator to the server you want to load the EPO Agent on
2. Click “Start”
3. Click “Run”
4. In the “Open” field, enter “\\<EPOServerName>\EPO-Agent” (for example, if your EPO Server is E000SUS1, you would enter \\E000SUS1\EPO-Agent)
5. Click “OK”
6. The EPO-Agent share should pop-up
7. In the EPO-Agent share, double click on “FramePkg” or “FramePkg.exe” (it is the same file, but Windows 2003 shows the extension)
8. A window should pop-up showing the progress of the EPO Agent installation
9. Once the agent has completed installing, the “OK” button should appear
10. Click the “OK” button in the EPO Agent Installation screen.

Setting up Network to Deploy ePolicy Orchestrator Agent

(Note: Once deployed, you may want to warn your users about how the Logon Script works and that their machine may reboot to load the agent software)

Setting Up Logon Script

1. Click on Start -> Run
2. In the “Open” field, enter “D:\Logon Scripts\”
3. If you do not have any Logon Scripts deployed, do the following:
 - a. Copy both the LOGON.BAT and EPO.BAT files to \\<DCName>\NETLOGON share (such as \\EDxxxxxxDI\NETLOGON)
 - b. Right click LOGON.BAT and choose “Properties”. Make sure that the Read-Only box is **Unchecked**.
 - c. Right click EPO.BAT and choose “Properties”. Make sure that the Read-Only box is **Unchecked**.
 - d. Right click EPO.BAT and click “Edit”
 - e. In the EPO.BAT, find each instance of “E000SUS1” and replace it with your EPO Server name (Note: There should be 5 instances of “E000SUS1” and you can use the search features in NotePad to help find them)
 - f. Save the changes and close the file
 - g. On your workstation, open “Active Directory Users and Computers” program
 - h. Find a test user account you can use and double click on the user
 - i. Go to the Profile tab
 - j. Under “User profile”, in the “Logon script” field, enter “Logon.bat (see example to the right)
 - k. Then click “OK”
 - l. Test the logon script by logging into various test machines at your site as this user and see if the Agent installs correctly
 - m. If the tests go well, open “Active Directory Users and Computers” program
 - n. Select all the user accounts you want to add the logon script to (be careful)
 - o. Right click and select “Properties”
 - p. Click on the “Profile” tab
 - q. Under “User profile”, check “Logon script”, and in the “Logon Script” field, enter “Logon.bat (see example to the right)
 - r. Click “OK” to make the changes
4. If a logon script is deployed that is just a batch file (such as Logon.bat), do the following:

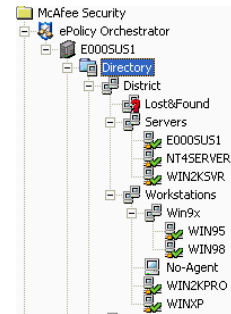


- a. Copy only EPO.BAT to [\\<DCName>\NETLOGON](#) share (such as [\\EDxxxxxxDI\NETLOGON](#))
 - b. Right click EPO.BAT and choose “Properties”. Make sure that the Read-Only box is **Unchecked**.
 - c. Right click EPO.BAT and click “Edit”
 - d. In the EPO.BAT, find each instance of “E000SUS1” and replace it with your EPO Server name (Note: There should be 5 instances of “E000SUS1” and you can use the search features in NotePad to help find them)
 - e. Save the changes and close the file
 - f. In the [\\<DCName>\NETLOGON](#) share, right click on the logon script batch file (such as Logon.bat), and click “Edit”
 - g. Enter “**CALL %0\..\EPO.BAT**” in each of the logon scripts being used.
(Note: this must be entered verbatim so it can load the EPO.BAT script)
Also, this line should be in the “LOGON.BAT” file in the “D:\Logon Scripts” directory to check for accuracy or to just copy and paste.
 - h. Save the changes to the file and close the file
5. If another product is being used (such as ScriptLogic or KiXtart), you should be able to easily integrate EPO.BAT into your logon scripts or copy the commands into your own scripts.
 6. If you have any questions, contact the KETS Help Desk or KETS Engineer

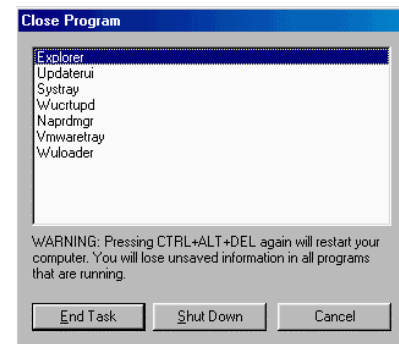
Verification of Services

Verifying ePolicy Orchestrator 3.0 Agent Installation

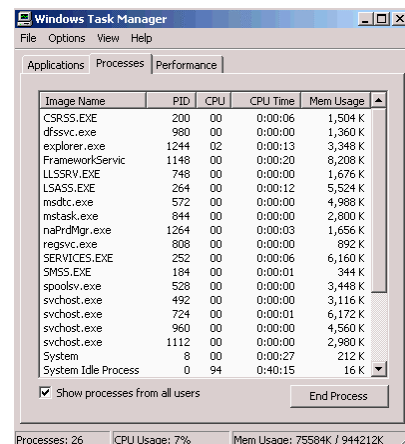
1. To check from the EPO Remote Management Console:
 - a. Open the EPO Remote Management Console and logon to your EPO Server
 - b. Expand the “Directory”
 - c. Expand the District Site
 - d. Expand “Servers”
 - e. Expand “Workstations”
 - f. Expand “Win9x”
 - g. All of the workstations and servers that have the agent loaded should be in the list with a green checkmark



2. To check from a Windows 95/98 workstation:
 - a. Press Ctrl-Alt-Delete
 - b. In the “Close Programs” screen, check the list for “Naprdmgr”
 - c. If “Naprdmgr” is in the list, then the EPO Agent is installed
 - d. If it is not present, try running the “DCOM95” for Windows 95 or “DCOM98” for Windows 98 (they are located on the EPO-Agent share). You will need to reboot the machine afterwards
 - e. Then from the EPO-Agent share, double click on “FramePkg” to manually reload the EPO Agent.



3. To check from a Windows NT/2000/XP/2003 machine:
 - a. Press Ctrl-Alt-Delete
 - b. Click on the “Task Manager” button
 - c. At the Task Manager screen, click on the “Processes” tab
 - d. At the bottom, check “Show processes from all users” if it is available
 - e. In the list, look for a service named “FrameworkService” on NT and 2000 machines or “FrameworkService.exe” on XP and 2003 machines
 - f. If it exists, the EPO Agent is loaded
 - g. If it does not exist, go to the EPO-Agent share and double click on “FramePkg” to manually load the EPO Agent.

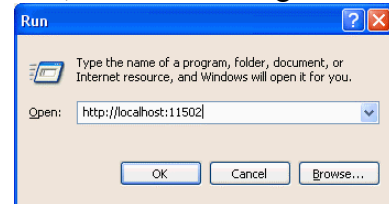


Checking the Status of the EPO Agent

Note: These are ways to see if an EPO Agent is communicating to the EPO Server and to check on the status of Policy, Product, and DAT updates. It can also be used to verify that the EPO Agent is loaded.

1. If you are at the workstation or server you want to check, do the following:

- a. Click on the “Start” button
- b. Click on “Run”
- c. In the “Open” field, enter <http://localhost:11502>
- d. Then click “OK”



- e. A browser window should pop-up with a list of recent communications between the EPO Agent and the EPO Server. The list starts with the oldest record and the most recent is at the bottom.

Date and Time	Type	Component	Message
Sunday, June 20, 2004 9:30:13 AM	Info	Internet Manager	Subsystem started
Sunday, June 20, 2004 9:30:14 AM	Info	Script	Subsystem started
Sunday, June 20, 2004 9:30:14 AM	Info	Update	Subsystem started
Sunday, June 20, 2004 9:30:14 AM	Info	Scheduler	Scheduler is now running
Sunday, June 20, 2004 9:30:14 AM	Info	Agent	Checking MAC address...
Sunday, June 20, 2004 9:30:14 AM	Info	Agent	Checking Computer Name...
Sunday, June 20, 2004 9:30:14 AM	Info	Agent	Generating Agent key pair...
Sunday, June 20, 2004 9:30:15 AM	Info	Agent	Generating Agent ID...
Sunday, June 20, 2004 9:30:15 AM	Info	Agent	Agent will connect to Server in randomized 10 minutes interval
Sunday, June 20, 2004 9:30:15 AM	Info	Agent	Agent will connect to Server in : 414 seconds
Sunday, June 20, 2004 9:30:15 AM	Info	Agent	Agent finished Enforcing policies
Sunday, June 20, 2004 9:30:15 AM	Info	Agent	Next policy enforcement in 5 minutes
Sunday, June 20, 2004 9:35:15 AM	Info	Agent	Agent Started Enforcing policies
Sunday, June 20, 2004 9:35:15 AM	Info	Management	Compiling policies
Sunday, June 20, 2004 9:35:15 AM	Info	Management	Enforcing Policies for EPOAGENT13000HETA
Sunday, June 20, 2004 9:35:15 AM	Info	Management	Enforcing Policies for EPOAGENT13000
Sunday, June 20, 2004 9:35:15 AM	Info	Management	Enforcing Policies for Policy Orchestrator Agent
Sunday, June 20, 2004 9:35:16 AM	Info	Agent	Agent finished Enforcing policies
Sunday, June 20, 2004 9:35:16 AM	Info	Agent	Next policy enforcement in 5 minutes
Sunday, June 20, 2004 9:37:09 AM	Info	Agent	Agent started performing ASCL
Sunday, June 20, 2004 9:37:09 AM	Info	Management	Collecting Properties
Sunday, June 20, 2004 9:37:11 AM	Info	Agent	Agent communication session started

2. If you want to remotely check the status of an EPO Agent, do the following:

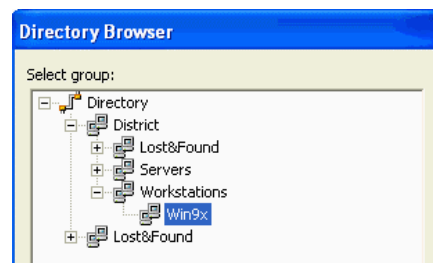
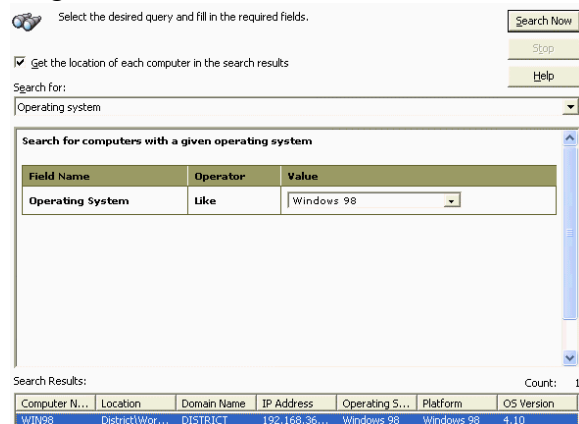
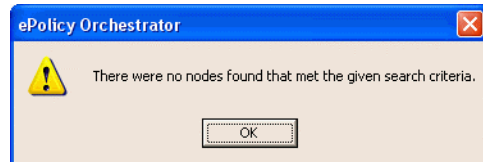
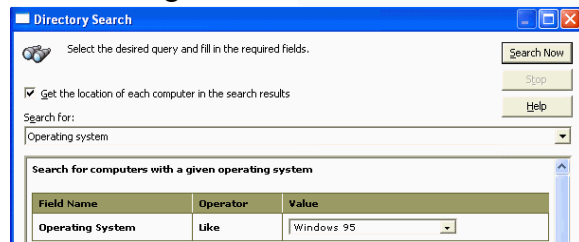
- a. Click on the “Start” button
- b. Click on “Run”
- c. In the “Open” field, enter **http://<Workstations_IP_Address>:11502**
- d. Then click “OK”
- e. The list of recent communications between the EPO Agent and the EPO Server should pop-up.

Maintenance Tasks

Searching and Moving Windows 9x machines to the Win9x Group

Note: This task moves computers from the Workstations group to the Win9x group so that VirusScan 4.5.1 can be installed on them. It is recommended that you run this regularly (once a week) to make sure that Windows 9x machines have the right policies.

1. Log into the EPO Server using the Remote Management Console
2. In the EPO Remote Management Console, right click on “Directory” and then click “Search...”
3. At the “Directory Search” screen, do the following:
 - a. Check “Get the location of each computer in the search results”
 - b. Under “Search for:”, click the drop down menu, scroll down, and click on “Operating System”
 - c. Once you click on “Operating System”, look at the three fields below “Field Name”, “Operator”, and “Value”
 - d. Under “Value”, click the drop down menu and select “Windows 95”
 - e. Click “Search Now”
 - f. If you get the error message, “There were no nodes found that met the given search criteria.”, then just click “OK” and you can go ahead and perform another search.
 - g. If you get results, then click on the first record under “Search Results”
 - h. Hold down the “Shift” key, then scroll down to the bottom of the list and click on the last record under “Search Results” (this should select all of the records in the list)
 - i. Right click the selected records and click on “Move To...”
 - j. The “Directory Browser” screen will pop up, double click on “Directory”, double click on the Directory Site, double click on “Workstations”, and click on “Win9x”
 - k. Click “OK” (then it is complete)



4. Repeat Step 3 and choose “Windows 98” instead of “Windows 95”
5. You can check to see if it worked by closing the “Directory Search” screen and going to the “Win9x” group and seeing if anything has been added
6. You can also check by doing the searches above (in Step 3) and instead of moving the computers, check the “Location” field at the bottom. All of them should have “<Directory Site>\Workstations\Win9x” in this field.
7. If they are all in the “Win9x” group, then it should be working.

Location
District\Workstations\Win9x\WIN98

Sorting Computers by IP Address

Note: This task sorts computers and moves them into the Server or Workstation group based on their IP address. This should automatically be done when the EPO Agent installs. However, if you run this task once a month, it will make sure that there are no computers kept in the “Lost & Found” directories.

1. Right click on “Directory” and choose “All Tasks”
2. Select “Sort Computers by IP...” from the list
3. At the “IP Sorting Wizard” screen, click “Next”
4. At the “IP Sorting Options” screen, do the following (these are the defaults):
 - a. Select “Leave them where they were found”
 - b. Check “Ignore machines with no IP address”
5. Click “Next” (it will start sorting, it may take a little time depending upon the number of computers in the Directory)
6. Once it is finished sorting, click “Next”
7. Click “Finish”